RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

FACULTAD INGENIERIA
PROGRAMA DE POSGRADO
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN Y ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN
BOGOTÁ D.C.

AÑO DE ELABORACIÓN: 2016

TÍTULO: DISEÑO DE UN PROGRAMA DE AUDITORÍA PARA LA ADMINISTRACIÓN, ASEGURAMIENTO Y CUMPLIMIENTO NORMATIVO DE LOS NÚMEROS DE IDENTIFICACIÓN PERSONAL - PIN EN ENTIDADES FINANCIERAS.

AUTOR (ES):

FORERO CRUZ William, HIDALGO LARA Pablo Andrés, MORA REYES Gustavo Adolfo y SABOGAL ZAMORA Adriana Carolina

DIRECTOR(ES)/ASESOR(ES):

Manuel Eberto Báez Mancera

MODALIDAD:

PÁGINAS: 104 **TABLAS:** 25 **CUADROS:** - **FIGURAS:** 17 **ANEXOS:** 10

CONTENIDO:

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE –	UNIVERSIDAD CATÓLICA de Colombia

PALABRAS CLAVES:

PLANEACIÓN, NORMAS, AUDITORIA, SEGURIDAD DE LA INFORMACION, PROGRAMA DE AUDITORÍA, ADMINISTRACIÓN, ASEGURAMIENTO Y CUMPLIMIENTO.

DESCRIPCIÓN: El proyecto de grado, propone realizar el diseño de un programa de auditoría para la administración, aseguramiento y cumplimiento normativo de los números de identificación personal- PIN en entidades financieras, teniendo en cuenta las normas PCI DSS2 , la ISO 9564 y a lo establecido por la SFC en la circular 029 de 2014, con el fin de coadyuvar mediante un programa establecido de auditoría a prevenir los riesgos relacionados con la información y el transporte electrónico de datos que se realizan a través de diversos dispositivos electrónicos, además de apoyar el cumplimiento de la misión y objetivos de estas organizaciones, procurando preservar las dimensiones de seguridad de la información (Integridad, Confidencialidad y Disponibilidad).

METODOLOGÍA: La metodología propuesta en el desarrollo del trabajo de grado está dividida en 4 fases que se llevaron a cabo de forma secuencial así:

Fase I. Definición de Requerimientos de Seguridad de Información y Cumplimiento Normativo de los Números de Identificación Personal – PIN que se deben evaluar en el Programa de Auditoría.

Fase II. Análisis de Riesgos relacionados con el Proceso de Administración, Aseguramiento y Cumplimiento Normativo de los Números de Identificación Personal – PIN.

Fase III. Diseño del Programa de Auditoría que permita evaluar el Cumplimiento Normativo y Seguridad de la Información sobre el servicio de Número de Identificación Personal - PIN.
Fase IV. Evaluar el Programa de Auditoría bajo un Mecanismo de Validación y Aprobación Seleccionado.

CONCLUSIONES:

Los requerimientos de seguridad identificados a partir de los estándares, normas nacionales e internacionales; permitieron identificar de forma clara y objetiva los

elementos más importantes del servicio de PIN , sobre los cuales se puede realizar la evaluación de auditoria en las entidades financieras.

El análisis de riesgos realizado, permitió establecer los activos de información, factores de riesgo y definir la metodología bajo la cual se identificarían, analizarían y priorizarían los riesgos asociados al PIN.

El programa diseñado permitió integrar los requerimientos de seguridad identificados con el análisis de riesgos, a fin de establecer las actividades y los detalles de evaluación del servicio de PIN.

La evaluación del programa a partir del juicio de expertos permitió incorporar el conocimiento y experiencia de personas que trabajan en el área de auditoria de sistemas o seguridad de la información que además conocen el servicio de PIN; con el fin de establecer oportunidades de mejora para fortalecer el alcance del programa.

Con el diseño del programa de auditoria las Entidades Financieras, contarán con herramientas de auditoría que permita a los auditores externos e internos y a los especialistas de seguridad de información establecer de forma objetiva pruebas de auditoria y/o revisiones de seguridad.

A través de la implementación del programa de Auditoria se apoyará a las entidades financieras en la disminución y prevención de fraudes relacionados con el robo de pines.

Se apoyará en la protección de las propiedades de información (Integridad, Confidencialidad y Disponibilidad) de las entidades financieras que utilicen el programa y a mejorar las condiciones actuales en materia de seguridad informática.

FUENTES:

Security Standards Council, LLC. (11 de 2013). Normas de seguridad de datos de la PCI PCI.

"Europay MasterCard VISA". (2010). EMV - Estándar de interoperabilidad de tarjetas IC ("Tarjetas con microprocesador") para la autentificación de pagos mediante tarjetas de crédito y débito.

© 2010 PCI Security Standards Council, LLC. (Septiembre de 2010). Aplicabilidad de laa norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) en un entorno EMV. En *Documento de Guía Borrador* (pág. Página 4).

A.C., I. m. (2004). Normas Internacionales de Auditoría. Mexico.

Amal Saha, S. S. (2011). Analysis of Applicability of ISO 9564 PIN based Authentication to Closed-Loop Mobile Payment Systems. 8.

Andreu, R. (1991). *Valor en la organizaciones* .

Asociación Bancaria Y De Entidades Financieras De Colombia. (2006). *ACUERDO INTERBANCARIO SEGURIDADES FÍSICAS Y DE LA INFORMACIÓN PARA CAJEROS AUTOMÁTICOS, PUNTOS DE VENTA Y TARJETAS DE CRÉDITO Y DÉBITO.* Bogotá D.C: ASOBANCARIA.

Asociación Española de Normalización y Certificación. (1999). *UNE-EN 29564-1: banca : gestión y seguridad del Número de Identificación Personal. Parte 1, Principios y técnicas de protección del PIN : (ISO 9564-1:1991).* AENOR.

Consejo Superior de Administración Electrónica. (2012). *Metodologia de análisis y gestión de riesgos de sistemas de información - MAGERIT.* España.

(1997). Coopers y Lybrand.

Davivienda. (04 de Febrero de 2016). *Quienes Somos*. Recuperado el 04 de Febrero de 2016, de https://www.davivienda.com/wps/portal/inversionistasespanol/inversionistas/AcercaBanco/quienes_somos/davivienda/

El Tiempo. (28 de enero de 2016). *eltiempo.com.* Recuperado el 8 de febrero de 2016, de eltiempo.com: http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

El tiempo- tecnosfera, R. (28 de 01 de 2016). En 2015, cibecrimen generó perdidas por US$ 600 millones en colombia. *El tiempo*, pág. 3.

Europay MasterCard VISA. (2010). EMV - Etándar de interoperabilidad de tarjetas IC ("Tarjetas con microprocesador") para la autentificación de pagos mediante tarjetas de crédito y débito.

http://www.asobancaria.com/. (Junio de 2006). Recuperado el 8 de febrero de 2016, de http://www.asobancaria.com/: http://www.asobancaria.com/portal/pls/portal/docs/1/4391771.PDF

Ieseinsight Business Knowledge Portal. (enero de 1991). Recuperado el 8 de febrero de 2016, de http://www.ieseinsight.com/: http://www.ieseinsight.com/fichaMaterial.aspx?pk=4318&idi=1&origen=1&idioma=1

Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. (2004). *NTC 2971. BANCA. ADMINISTRACION Y SEGURIDAD DEL NUMERO DE IDENTIFICACION PERSONAL. NIP - PIN -.* Colombia: ICONTEC.

ISO - International Organization for Standardization. (2011). *Standard 9564-1: 2011, Financial services -- Personal Identification Number (PIN) management and security*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54083

Le-Fort, S. C. (8 de Junio de 2010). *Superintendencia de bancos e instituciones financieras de chile.* Recuperado el 17 de Febrero de 2016, de Superintendencia de bancos e instituciones financieras de chile: http://www.sbif.cl/sbifweb/internet/archivos/DISCURSOS_9296.pdf

Librand, C. y. (1997).

LLC-Security Standards Council. (11 de 2013). Normas de seguridad de datos de la PCI PCI.

MARTÍN, S. G. (2009). Personalización y autorización de tarjetas de crédito de tarjetas de crédito. *TRABAJO FIN DE CARRERA* . Madrid.

PCI Security Standards Council. (14 de Septiembre de 2010). *Aplicabilidad de la norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) en un entorno EMV*. Obtenido de https://www.pcisecuritystandards.org/documents/pci_dss_emv-es.pdf

PIATTINI, M. y. (1998). *Auditoría Informatica.* Bogotá: Alfaomega.

Pontificia Universidad Javeriana -Velandia Sosa. (2013). *La auditoría de sistemas como apoyo a la revisoría fiscal.* Bogotá.

Shier, J. (18 de Abril de 2014). *PCI DSS – ¿Qué hay de nuevo en la versión 3.0?* Obtenido de Naked Security By Sophos: https://nakedsecurity.sophos.com/es/2014/04/18/pci-dss-whats-new-in-v3-0/

Standardization, I. O. (2011). Norma ISO 19011.

Standardization, I. O. (2011). Norma ISO 19011 - Directrices para la auditoría de Sistemas de Gestión.

Superintendencia financiera de Colombia. (2014). Circular 029 de 2014, parte 1, titulo II (Canales, medios, seguridad y calidad en el manejo de la información en la prestacion de servicios financieros). Bogotá, Colombia.

Superintendencia Financiera de Colombia. (OCTUBRE de 2014). *SUPERINTENDENCIA FINANCIERA DE COLOMBIA* . Obtenido de ttps://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=10083443

UNINFO (Tecnologías de la Información y sus aplicaciones) . (Martes 28 de Junio de 2011). *Uni Ente Italiano Di Normazione.* Obtenido de https://translate.google.com.co/translate?hl=es&sl=it&tl=es&u=http%3A%2F%2Fwww.uni.com%2Findex.php%3Foption%3Dcom_content%26view%3Dfeatured%26Itemid%3D84https://translate.google.com.co/translate?hl=es&sl=it&tl=es&https://translate.google.com.co/translate?

VISA. (12 de Febrero de 2013). *Seminarios por Internet para Destacar la Seguridad del PIN y de los Datos del Tarjetahabiente por parte de los Comercios.*

Security Standards Council, LLC. (11 de 2013). Normas de seguridad de datos de la PCI PCI.

"Europay MasterCard VISA". (2010). EMV - Estándar de interoperabilidad de tarjetas IC ("Tarjetas con microprocesador") para la autentificación de pagos mediante tarjetas de crédito y débito.

© 2010 PCI Security Standards Council, LLC. (Septiembre de 2010). Aplicabilidad de laa norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) en un entorno EMV. En *Documento de Guía Borrador* (pág. Página 4).

A.C., I. m. (2004). Normas Internacionales de Auditoría. Mexico.

Amal Saha, S. S. (2011). Analysis of Applicability of ISO 9564 PIN based Authentication to Closed-Loop Mobile Payment Systems. 8.

Andreu, R. (1991). *Valor en la organizaciones .*

Asociación Bancaria Y De Entidades Financieras De Colombia. (2006). *ACUERDO INTERBANCARIO SEGURIDADES FÍSICAS Y DE LA INFORMACIÓN PARA CAJEROS AUTOMÁTICOS, PUNTOS DE VENTA Y TARJETAS DE CRÉDITO Y DÉBITO.* Bogotá D.C: ASOBANCARIA.

Asociación Española de Normalización y Certificación. (1999). *UNE-EN 29564-1: banca : gestión y seguridad del Número de Identificación Personal. Parte 1, Principios y técnicas de protección del PIN : (ISO 9564-1:1991).* AENOR.

Consejo Superior de Administración Electrónica. (2012). *Metodologia de análisis y gestión de riesgos de sistemas de información - MAGERIT.* España.

(1997). Coopers y Lybrand.

Davivienda. (04 de Febrero de 2016). *Quienes Somos*. Recuperado el 04 de Febrero de 2016, de https://www.davivienda.com/wps/portal/inversionistasespanol/inversionistas/AcercaBanco/quienes_somos/davivienda/

El tiempo- tecnosfera, R. (28 de 01 de 2016). En 2015, cibecrimen generó perdidas por US$ 600 millones en colombia. *El tiempo*, pág. 3.

Europay MasterCard VISA. (2010). EMV - Etándar de interoperabilidad de tarjetas IC ("Tarjetas con microprocesador") para la autentificación de pagos mediante tarjetas de crédito y débito.

http://www.asobancaria.com/. (Junio de 2006). Recuperado el 8 de febrero de 2016, de http://www.asobancaria.com/: http://www.asobancaria.com/portal/pls/portal/docs/1/4391771.PDF

Ieseinsight Business Knowledge Portal. (enero de 1991). Recuperado el 8 de febrero de 2016, de http://www.ieseinsight.com/: http://www.ieseinsight.com/fichaMaterial.aspx?pk=4318&idi=1&origen=1&idioma=1

Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. (2004). *NTC 2971. BANCA. ADMINISTRACION Y SEGURIDAD DEL NUMERO DE IDENTIFICACION PERSONAL. NIP - PIN -.* Colombia: ICONTEC.

ISO - International Organization for Standardization. (2011). *Standard 9564-1: 2011, Financial services -- Personal Identification Number (PIN) management and security*. Obtenido de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54083

Le-Fort, S. C. (8 de Junio de 2010). *Superintendencia de bancos e instituciones financieras de chile.* Recuperado el 17 de Febrero de 2016, de Superintendencia de bancos e instituciones financieras de chile: http://www.sbif.cl/sbifweb/internet/archivos/DISCURSOS_9296.pdf

Librand, C. y. (1997).

LLC-Security Standards Council. (11 de 2013). Normas de seguridad de datos de la PCI PCI.

MARTÍN, S. G. (2009). Personalización y autorización de tarjetas de crédito de tarjetas de crédito. *TRABAJO FIN DE CARRERA* . Madrid.

PCI Security Standards Council. (14 de Septiembre de 2010). *Aplicabilidad de la norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) en un entorno EMV*. Obtenido de https://www.pcisecuritystandards.org/documents/pci_dss_emv-es.pdf

PIATTINI, M. y. (1998). *Auditoría Informatica.* Bogotá: Alfaomega.

Pontificia Universidad Javeriana - Néstor Orlando Velandia Sosa. (2013). *La auditoría de sistemas como apoyo a la revisoría fiscal.* Bogotá.

Shier, J. (18 de Abril de 2014). *PCI DSS – ¿Qué hay de nuevo en la versión 3.0?* Obtenido de Naked Security By Sophos: https://nakedsecurity.sophos.com/es/2014/04/18/pci-dss-whats-new-in-v3-0/

Standardization, I. O. (2011). Norma ISO 19011.

Standardization, I. O. (2011). Norma ISO 19011 - Directrices para la auditoría de Sistemas de Gestión.

Superintendencia financiera de Colombia. (2014). Circular 029 de 2014, parte 1, titulo II (Canales, medios, seguridad y calidad en el manejo de la información en la prestacion de servicios financieros). Bogotá, Colombia.

Superintendencia Financiera de Colombia. (OCTUBRE de 2014). *SUPERINTENDENCIA FINANCIERA DE COLOMBIA* . Obtenido de ttps://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=10083443

Tiempo, E. (28 de enero de 2016). *eltiempo.com.* Recuperado el 8 de febrero de 2016, de eltiempo.com: http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

UNINFO (Tecnologías de la Información y sus aplicaciones) . (Martes 28 de Junio de 2011). *Uni Ente Italiano Di Normazione.* Obtenido de https://translate.google.com.co/translate?hl=es&sl=it&tl=es&u=http%3A%2F%2Fwww.uni.com%2Findex.php%3Foption%3Dcom_content%26view%3Dfeatured%26Itemid%3D84https://translate.google.com.co/translate?hl=es&sl=it&tl=es&https://translate.google.com.co/translate?

VISA. (12 de Febrero de 2013). *Seminarios por Internet para Destacar la Seguridad del PIN y de los Datos del Tarjetahabiente por parte de los Comercios.*

LISTA DE ANEXOS:

ANEXO 1- Glosario
ANEXO 2 - Matriz V3 – Req Seguridad – PIN
ANEXO 3 - Matriz de riesgos
ANEXO 4 - Matriz de riesgos programa
ANEXO 5 - Formato de Muestreo
ANEXO 6 - Programa de auditoría.
ANEXO 7 - Formato de validación del programa de auditoría. (Jorge Zipa)
ANEXO 8 - Formato de validación del programa de auditoría. (José Marín)
ANEXO 9 - Carta de validación del programa de auditoría (Jorge Zipa)
ANEXO 10 - Carta de validación del programa de auditoría (José Marín)